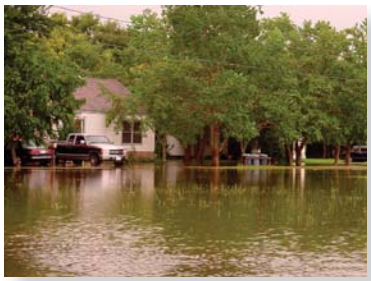
ACN*Report*

Summer 2005 Vol. IV, No. 2

A National Security and Emergency Preparedness (NS/EP) Support Program of the National Communications System

ACN Supports Katrina Relief



Disaster can strike at any time without warning. In late August, Hurricane Katrina slammed into the United States, ravaging communities in Florida, Alabama, Georgia, Louisiana, and Mississippi. In its wake, the country found itself trying to put the pieces back together.

The ability to communicate effectively during such incidents of national significance is crucial to any relief efforts. In this case, however, the devastated regions reported over 600 thousand power outages, making efficient communication difficult. As such, a portion of the National Communications System's (NCS) contingency plan relied on the Alerting and Coordination Network (ACN), which remained operational during the hurricane.

continued on page 3

Exercise PINNACLE

In the aftermath of Hurricane Katrina, it is evident that the need for quick, reliable lines of communication can arise without warning. Every now and then, a catastrophic incident reminds us how vital it is to have dependable continuity of operations (COOP) plans. Fortunately, when Katrina struck the Gulf Coast in late August, the Alerting and Coordination Network (ACN) was ready to react and played an integral role in supporting relief efforts (see *Katrina*, this page). The network's effectiveness during such incidents of national significance is due in large part to Federal Government exercises. From June 21 through June 24, ACN, under the Department of Homeland Security (DHS), participated in Exercise PINNACLE, an event that tested the Federal Government's ability to operate during incidents of national significance.

DHS was one of several Federal departments and agencies involved in PINNACLE. During the exercise, participants took part in a hypothetical terrorism scenario requiring the Federal Government to conduct contingency activities.

continued on page 2

In This Issue

Read the Conference Call Procedures on Page 4

Monthly Voice Test Calls

On the 15th* of every month, Alerting and Coordination Network (ACN) administrators conduct a network-wide conference call to test ACN's conference bridge capabilities. Administrators initiate this test call between 1:00-1:30 PM EST on the day of the test. Maximum membership participation is imperative in order to accurately evaluate ACN's conference bridge. ACN administrators send out reminder e-mails to all members one week prior to the monthly tests. Please make every effort to ensure the personnel responsible for monitoring the ACN phone prepare for and respond to the conference call.

It is important to note that, in addition to the conference call, administrators also conduct individual ring-down test calls to all members on the 15th* of the month. These separate calls occur between the hours of 9:00 AM and 5:00 PM EST.

It is important to answer both test calls. Thank you in advance for your cooperation.

**If the 15th falls on a weekend, the test calls occur on the following Monday.*

From Spam to SPIT

Brian J. Forbes
Technical Writer

Believe it or not, junk mail is actually beginning to develop a vast lineage. Sure, it all started with unwanted envelopes showing up in mailboxes across the country, but it has become so much more than that. Telemarketing calls interrupt our dinners, and spam bombards our e-mail accounts. Banner ads pop up and obstruct our favorite Web sites. More recently, SPIM, or spam over instant messaging, invaded the world of instant messaging. It seemed only a matter of time before junk mail caught up with voice over Internet protocol (VoIP).

Which brings us to SPIT. SPIT is spam over Internet protocol telephony. Also known as VAM (voice or VoIP spam), SPIT is telemarketing voicemail blasted out simultaneously to millions of Internet phone users. Marketers are excited about the newfound opportunities, because the technology behind VoIP allows them to send messages in bulk rather than dial numbers individually. All this equates to what could possibly be a rather large monkey wrench thrown into the heart of the VoIP industry.

The good news is that, as VoIP has yet to find its niche in mainstream Americana, SPIT is not creating too much havoc yet. Even better, although the Alerting and Coordination Network (ACN) does rely primarily on VoIP, it rides over a privately-managed network. This makes the likelihood of ACN becoming susceptible to SPIT virtually impossible.

You should be aware, however, that since ACN has a connection to the public switched network, a telemarketer could conceivably reach you by dialing your ACN phone number. ACN administrators are mitigating this predicament the best way possible: they are not publishing your ACN number. In fact, no where can potential spammers find a publicly published ACN User Directory, because such a directory does not exist.

If you ever do receive a call from a telemarketer or anyone that does not belong to ACN, please take down the number (as well as the caller's name and employer, if possible), and then notify the ACN Help Desk immediately. Given that information, administrators will configure ACN's voice firewall to block that specific number from ever dialing anyone on the network again.

The intrusions never stop. First marketers hit us with junk mail. Then they unveiled spam. And now they have come up with SPIT.

Some people just don't have any manners.

PINNACLE *continued from page 1*

Various organizations implemented COOP plans and assessed communications connectivity, validating the Government's ability to continue essential operations during threats and emergencies.

In an article published in *DHS Today*, Homeland Security Secretary Michael Chertoff stressed the importance of exercises such as PINNACLE. "Assuring the ability of the Federal Government to continue its essential functions is good government," said Chertoff. "Threat situations, domestic attacks, and natural disasters all present challenges to our Federal operations, and Exercise PINNACLE provides a demanding scenario to test our essential functions and assure their continuation."

Exercise PINNACLE focused on testing Federal Government operations and procedures during real-life circumstances and ACN played a role in the exercise. The National Coordinating Center for Telecommunications (NCC) Watch successfully validated connectivity and communications with ACN's COOP site during PINNACLE. ACN looks forward to participating in future readiness exercises as circumstances permit, as involvement in this type of training helps ensure that ACN stays mission-ready at all times.

Mr. Forbes is a Technical Writer for Arrowhead Global Solutions, under contract to the NCS.

ACN Extension Change

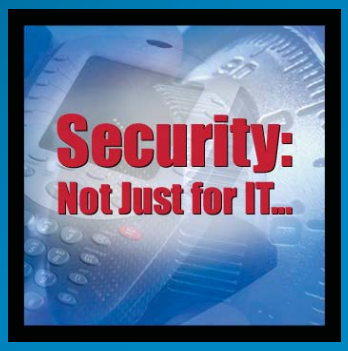
Albert Einstein once said that progress is impossible without change. If that is true, then the Alerting and Coordination Network (ACN) just took another step forward. During the summer, you probably noticed a slight but significant modification to your ACN phone: your four-digit phone number extension changed.

In order to grant ACN members inbound and outbound connectivity with the public switched network (PSN), administrators needed to modify all ACN extensions so that they match the last four digits of the new PSN numbers. The change only affected one of the four digits that made up your original number. The old ACN extensions began with a 52. The new extensions start with a 50.

The transition to new extensions went smoothly, as 95 percent of the updated phone numbers were in place by the end of August. Administrators will send you an updated version of the ACN directory this Fall.

The Enemy Within

Christopher Leverich
Security Analyst



There is an old adage that goes something like this: "Help defend me from my friends; from my enemies I can defend myself." It may be dated, but the message still rings true today. How so? The finest computer security that money can buy protects your network from outside intrusion, but inside your office walls, it may be open season. What are we getting at? In a word: espionage.

Espionage is the practice of spying or using spies to obtain information about plans and activities. And more often than not, the guilty party is operating right under your nose. Espionage is not contingent upon the presence of a distant enemy. All it needs is an insider with a willingness to betray.

According to a report on the Defense Security Service (DSS) Internet Web site, 79 percent of all Americans arrested for espionage during the past 55 years volunteered their services to foreign intelligence agencies without solicitation. It makes sense: buyers of protected records take great risks trying to locate and contact a willing seller privy to the desired information. A willing seller, however, has much less chance of getting caught. An increasingly interconnected world makes it easier for sellers to identify and contact potential buyers.

Persons intending to commit espionage can operate in a number of different ways. They can "dumpster dive" through trash to gather sensitive documentation improperly discarded. They might use commercially available listening devices (such as police scanners) to eavesdrop on classified conversations behind closed boardroom doors. Social engineering is also a popular technique. What might seem like harmless banter to you may very well be someone else's scheme to elicit confidential material. More sophisticated criminal masterminds may even infiltrate data-storing cache chips on fax machines and laptops.

Or maybe the guilty culprit will not have the need to use any of the above. Perhaps he is a long-term employee who has gained the trust and confidence of his co-workers. And as appalling as it may be, one day he simply decides to betray that confidence by selling the very information he has been entrusted to protect.

But while the means may vary, the end result rarely does: espionage provides unauthorized intelligence services and/or terrorist groups sensitive information about your organization.

What to watch out for? There are four basic conditions that need to exist for John Doe to commit espionage. He needs an opportunity to commit the crime. He needs a motive. He has to have the capacity to disregard inhibitors such as morals, loyalty, and fear. Lastly, there has to be an action or activity that triggers the betrayal.

Counter-intelligence agencies such as the Federal Bureau of Investigation (FBI) have methods of surveillance used to detect suspicious activity. Chances are you don't have a covert FBI agent patrolling your hallways, however. Nevertheless, you should report any or all strange activities to your facilities security officer.

The best preventative technique is situational awareness. Ensure sensitive information and equipment (like your Alerting and Coordination Network phone) are properly controlled. And be mindful of the folks who share your workspace.

Thankfully, it is not easy for offenders to conduct business. Over one quarter of those arrested for espionage since 1950 did not successfully compromise secure information, as authorities caught them in the act. Police apprehended an additional 27 percent of espionage criminals during their first year of operation.

As human beings, we may very well be our own worst enemies. Fortunately, when properly informed, we are also our own best security system.

Mr. Leverich is a Security Analyst for Arrowhead Global Solutions, under contract to the NCS.

Katrina *continued from page 1*

In the first two weeks following Katrina, the NCS averaged two to three conference calls per day via ACN. In some instances, over 40 ACN members participated in a given call. Subjects of discussion included highway accessibility, driver security, diesel fuel availability, and restoration/re-supply. ACN's conference bridge performed admirably during these calls, providing steadfast lines of communication with excellent audio quality.

ACN's mandate is to provide connectivity when regular forms of communication are inoperable. During the Katrina restoration effort, the network once again proved to be a valuable asset. ACN remains resolute in its ability to offer the Nation a stable communication option in times of need.

Conference Call Procedures:

- The conference bridge rings all members simultaneously.
- When you answer, **please wait** until the automated voice prompts you to enter your Personal Identification Number (PIN).
- There may be up to a 15-second delay before the prompt.
- There is no audible indicator that you are on hold.
- Enter your PIN, followed by the pound (#) sign. Your PIN is your ACN extension followed by the last two digits of your extension a second time. For instance, extension 5296 has a PIN of 529696#.
- Officially announce your presence upon joining the call.

Please call the ACN Help Desk with any questions.

Mind Bender

Have some fun! Write your answers in order in the spaces below.

? the number of ACN newsletters you would expect to receive over two years

? the first two digits of the ACN Help Desk extension

? the number of different ACN members (not sites) at the end of 2004 (two digits)

? the number of titles listed in the table of contents of this newsletter, minus 2

? ”P” on your ACN phone

? the last digit of the NCS P.O. Box

? “Q” on your ACN phone

? the number of titles listed in the table of contents of the previous ACN newsletter

? “R“ on your ACN phone

? the current ACN newsletter volume number x 2

___ ___ _____

Now use the keypad of your ACN phone to help determine a corresponding letter for each number and enter it below. The correct letters spell an item that all ACN members are familiar with. The answer will be revealed in the next issue. Good luck!

___ ___ _____

ACN Program Management Office

Tel: 1-866-NCS-CALL (1-866-627-2255)
1-703-676-CALL (703-676-2255) DC Metro Area
E-mail: acn@dhs.gov
Web: www.ncs.gov/acn

Department of Homeland Security
Information Analysis and Infrastructure Protection Directorate
National Communications System
P.O. Box 4502
Arlington, VA 22204-4502

Technical Support: ACN Help Desk

ACN Ext: 4357 (HELP)
Tel: 1-877-441-9330 (Toll Free)
E-mail: smc@arrowhead.com

24/7 ACN Help Desk:
1-877-441-9330

Monthly Test
1:00-1:30 PM EST
15th of the month,
or the following Monday